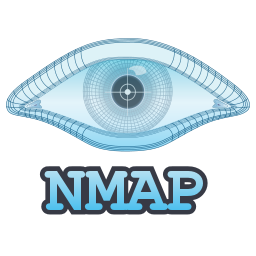
**Assignment No :- 6**

**Aim :-** Demonstrate the NMAP tool, tcp dump and observe data transferred in client server communication.

**Introduction:-**

****

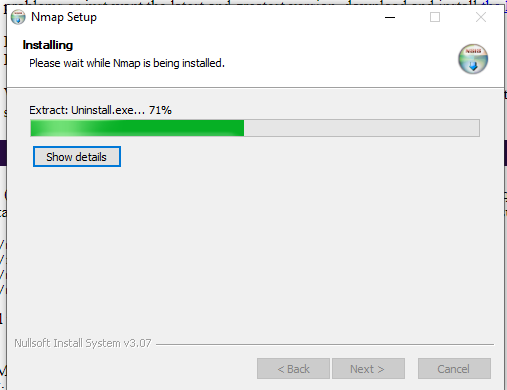
Nmap is a network scanning tool that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.

The program is most commonly used via a command-line interface (though GUI front-ends are also available) and is available for many different operating systems such as Linux, Free BSD, and Gentoo. Its popularity has also been bolstered by an active and enthusiastic user support community.Nmap was developed for enterprise-scale networks and can scan through thousands of connected devices. However, in recent years Nmap is being increasingly used by smaller companies. The rise of the IoT, in particular, now means that the networks used by these companies have become more complex This means that Nmap is now to audit the traffic between web servers and IoT devices. The recent emergence of has also stimulated interest in Nmap, not least because of its ability to interrogate and to highlight any devices that may be malicious.

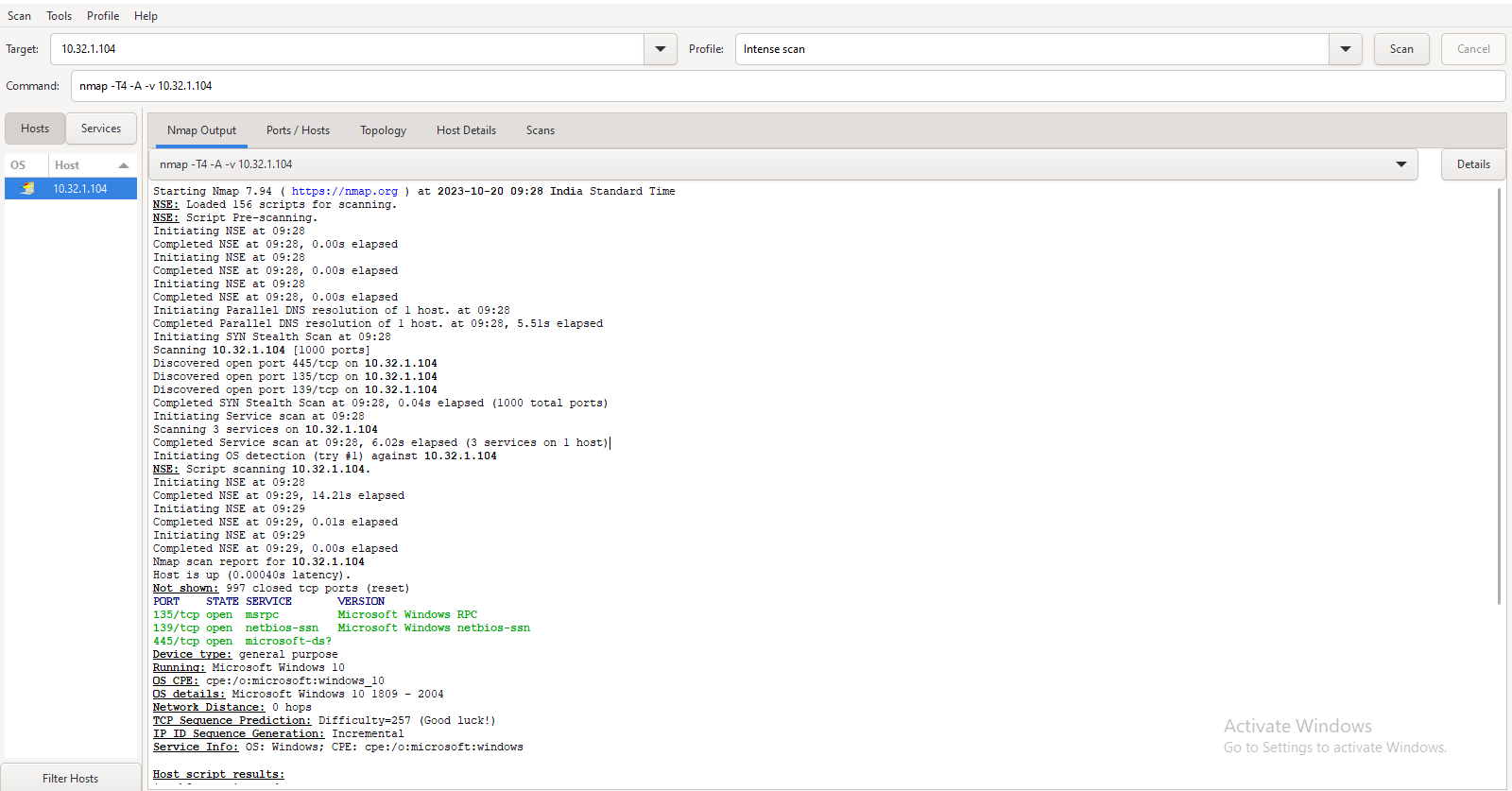
**Steps to install and run the NMAP:-**

**Step 1 :-** Go to the official website of NMAP and Click on download NMAP.

Download the all required packages and dependencies

****

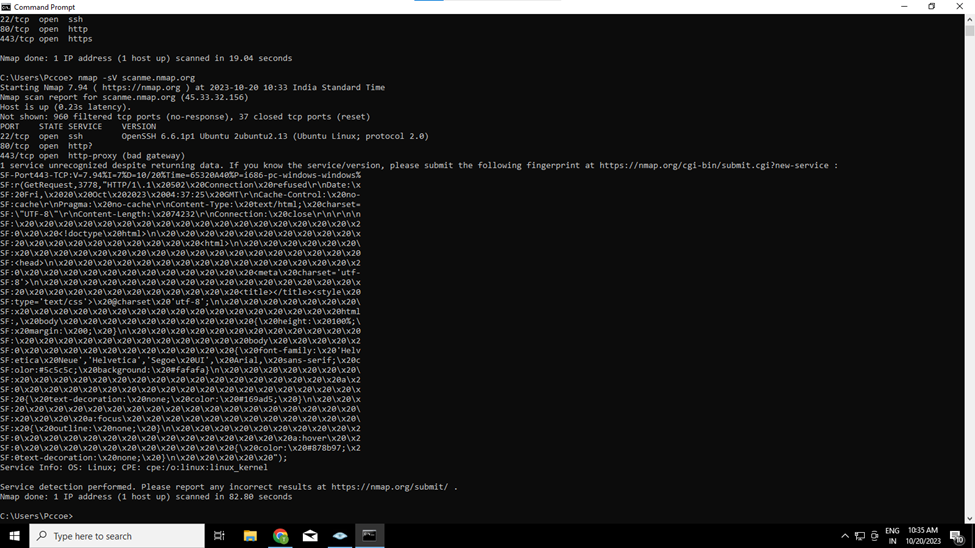
**Step 2 :-** Start the Nmap and apply the filters



1)**Version scanning**

Nmap (Network Mapper) is a powerful open-source network scanner used for network discovery and security auditing. It's capable of performing various types of scans to gather information about target hosts.One of the fundamental tasks in Nmap is version scanning, which aims to determine the version and service information of open ports on a target system. This helps in identifying vulnerable services that might be running.

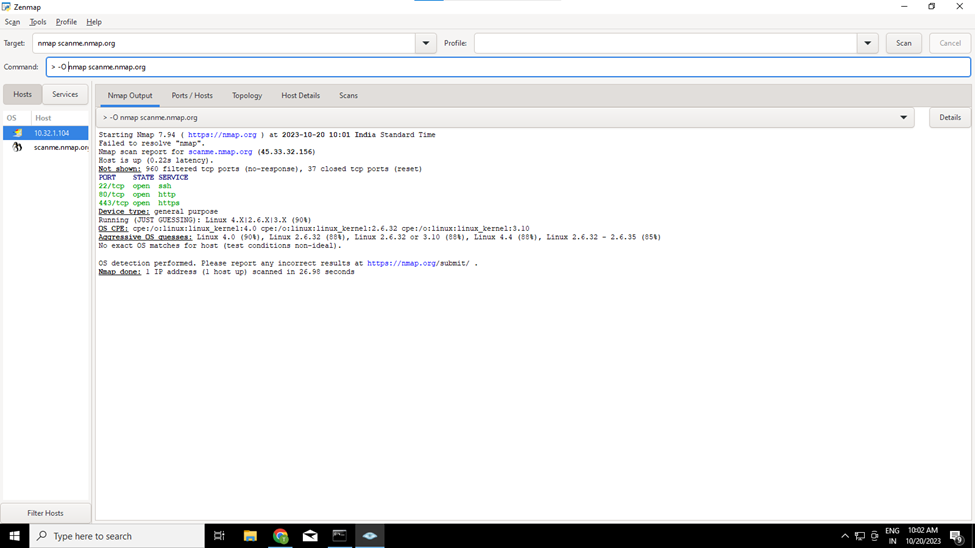
**>** nmap -sV target



**2)OS Scanning:**

In addition to the services and their versions, Nmap can provide information about the underlying operating system using TCP/IP fingerprinting. Nmap will also try to find the system uptime during an OS scan.

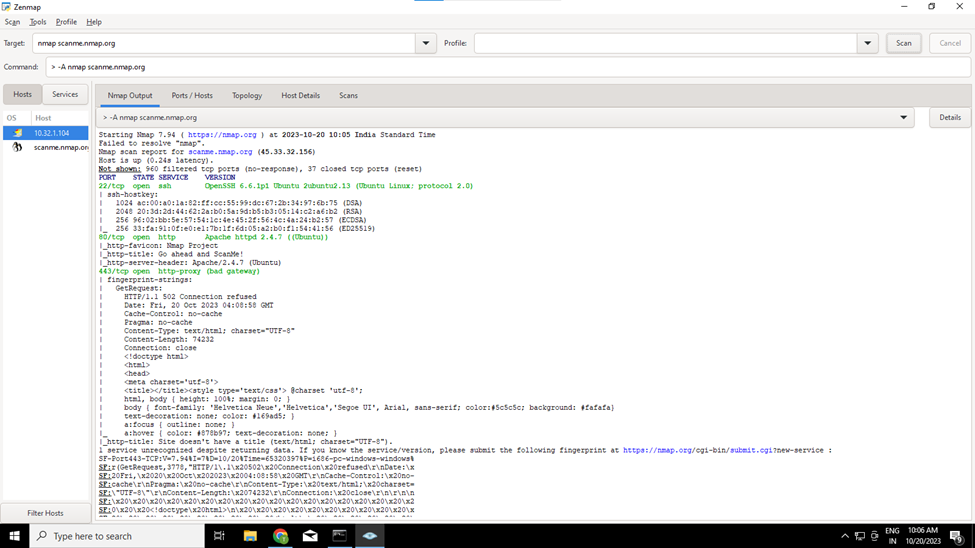
> nmap -O scanme.nmap.org

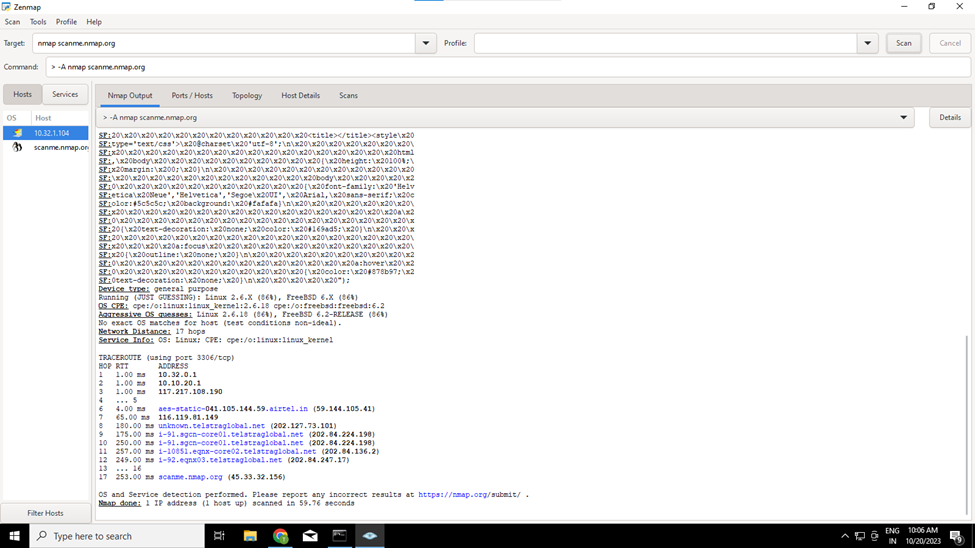


**3)Aggressive Scanning:**

Nmap has an aggressive mode that enables OS detection, version detection, script scanning, and traceroute. You can use the -A argument to perform an aggressive scan.

> nmap -A scanme.nmap.org

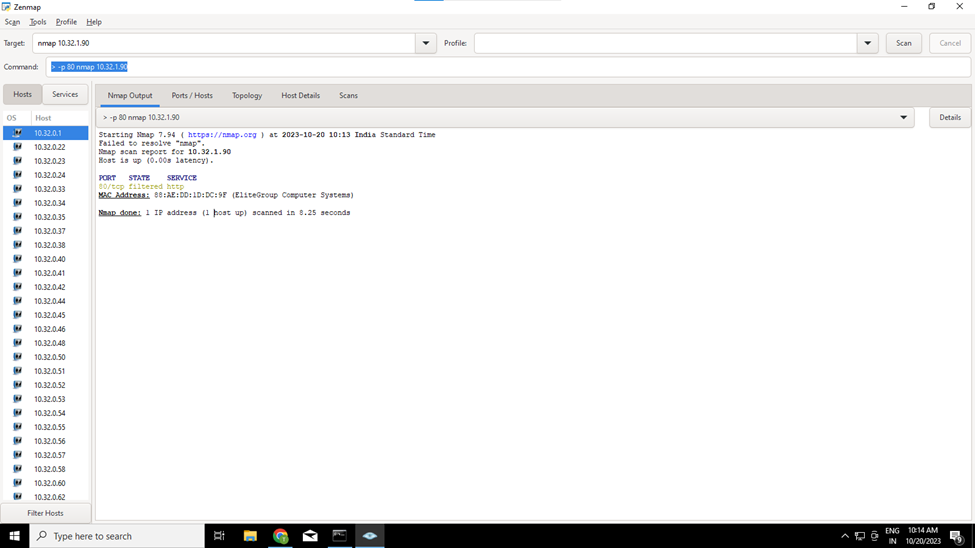


****

**4)Port Scanning**

Port scanning is one of the most fundamental features of Nmap.

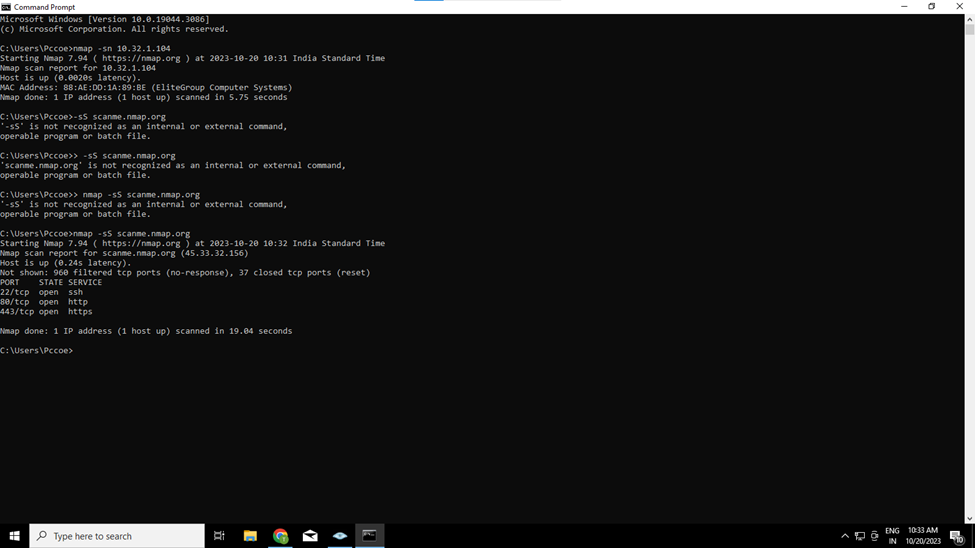
> -p 80 nmap 10.32.1.90

****

**2.Stealth scan:**

Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

> nmap -sS scanme.nmap.org



**Features :-**

1. **Host Discovery:**

Nmap can determine which hosts are available on a network and their respective IP addresses.

1. **Port Scanning:**

It can scan for open ports on a target host, which is crucial for identifying services that are running.

1. **Service Detection:**

Nmap can determine the services and applications running on open ports, providing information on their versions.

1. **Operating System Detection:**

It has the capability to identify the operating system running on a target host based on the network responses.

1. **Scripting Engine (NSE):**

Nmap comes with a powerful scripting engine that allows users to write custom scripts to automate various tasks and perform advanced network scanning techniques.

1. **Version Detection:**

It can detect specific versions of services and applications running on open ports, which is essential for vulnerability assessment.

**Advantages of NMAP:**

1. **Comprehensive Network Scanning:** Nmap provides a wide range of scanning techniques to gather detailed information about hosts and services on a network.
2. **Open Source and Free**: Nmap is open-source software, which means it's freely available for anyone to use, modify, and distribute.
3. **Cross-Platform Compatibility:** Nmap is designed to work on multiple operating systems including Windows, Linux, macOS, and others, making it a versatile tool**.**
4. **Highly Customizable:** Users can tailor scans to their specific needs by adjusting parameters like scan type, timing options, and target specification.
5. **Scripting Engine (NSE):** The Nmap Scripting Engine allows users to write custom scripts to automate tasks and perform advanced scanning techniques.
6. **Efficiency and Performance Optimization:** Nmap is optimized for performance and can handle large numbers of hosts and ports. It offers options for fine-tuning scan speed and parallelization.
7. **Network Topology Mapping:** Nmap can create visual representations of the network topology, which is useful for understanding how hosts are interconnected.

**Disadvantages :-**

1. **Learning Curve:** Nmap can be complex for beginners, and users may require time and effort to become proficient in using all of its features effectively.
2. **Legal and Ethical Considerations:** Using Nmap for network scanning without proper authorization can be illegal and unethical. Always ensure you have the appropriate permissions before conducting any scanning activities.
3. **Potential for False Positives/Negatives:** Depending on network conditions and configurations, Nmap may produce inaccurate results, including false positives (indicating services that aren't actually present) or false negatives (missing actual services).
4. **Resource Intensive:** Intensive scans on large networks can consume significant system resources, potentially impacting network performance.
5. **Firewall and IDS Evasion Techniques:** While Nmap provides techniques for evading firewalls and intrusion detection systems, it's important to use these features responsibly and in compliance with legal and ethical standards.

**Applications :-**

1. **Network Discovery:**

Identifying hosts and devices on a network, including their IP addresses and MAC addresses.

1. **Port Scanning:**

Determining which ports are open on a host, which services are running, and the version of those services.

1. **Service Detection:**

Identifying the specific services and applications that are running on open ports, along with their versions.

1. **Operating System Detection:**

Determining the operating system (OS) running on a target host based on the network responses.

1. **Vulnerability Assessment:**

Identifying potential security vulnerabilities by discovering open ports and services that may be susceptible to known exploits.

1. **Firewall Testing:**

Evaluating the effectiveness of firewalls and intrusion detection systems by attempting to bypass them using Nmap's evasion techniques.

1. **Security Auditing:**

Performing comprehensive scans to assess the security posture of a network, including identifying weak points and potential entry points for attackers.

**Conclusion:-**

In conclusion, Nmap stands as a versatile and powerful network scanning tool, playing a pivotal role in network security, discovery, and vulnerability assessment. Its features, ranging from host discovery and port scanning to service and operating system detection, make it an indispensable asset for both large enterprises and smaller organizations. The tool's open-source nature, cross-platform compatibility, and a rich set of features, such as the Nmap Scripting Engine (NSE), contribute to its widespread adoption in the cybersecurity community.